SEARCH NOTES

09/702,728

WEST Search History

DATE: Tuesday, November 04, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=OR		
L20	L19 and l18	54	L20
L19	(reduc$ or prevent$ or avoid$) near9 (fraud$ or delinquent)	2708	L19
L18	L17 and l16	163	L18
L17	(late or fail$ or fraud$) near7 (pay$ or paid or payment) or delinquent	1789	L17
L16	L15 same l14	2103	L16
L15	credit near5 card	15596	L15
L14	track$ or review$ or monitor$ or creen$	750557	L14
L13	L12 and l11	32	L13
L12	credit near7 history	447	L12
L11	L10 and l9	126	L11
L10	(increas$ or extend$ or expand$) near9 limit	69202	L10
L9	L8 and l7	1929	L9
L8	credit near7 (limit or line)	2601	L8
L7	credit near7 card	15654	L7
L6	L5 and l4	23	L6
L5	credit near7 limit$	1859	L5
L4	L3 and l1	85	L4
L3	(late$ or bad$)near7 payment	477	L3
L2	late$ near7 payment	443	L2
L1	(monitor$ or track$ or screen$)near7 account	4890	L1

END OF SEARCH HISTORY

WEST

Generate Collection Print

L18: Entry 43 of 163 File: USPT Nov 20, 2001

DOCUMENT-IDENTIFIER: US 6321206 B1
TITLE: Decision management system for creating strategies to control movement of clients across categories

Brief Summary Text (21):
From step 60, the system moves to step 70, where inbound events are matched to processes. More specifically, it is defined which processes are invoked in response to each inbound event. For example, different processes are created for a credit card campaign versus a late payment. The order of process execution is also specified.

Brief Summary Text (28):
Similarly, referring now to FIG. 4(B), for example, when an inbound event 96 is a late payment, the following processes are applied, in order: risk score 97, underwriting treatment 98 and overdraft decision treatment 99. A result 100 of the applied processes is a determination whether to send new underwriting and overdraft codes.

Brief Summary Text (43):
Moreover, the above-described decision management system will not provide a mechanism for monitoring performance and developing strategies which effectively move customers from one category to another. For example, the decision management system will not allow a credit card company to monitor performance and effectively develop strategies to move customers from the Silver category to the Gold category.

Detailed Description Text (30):
On Jan. 31, 1998, Feb. 31, 1998, Mar. 31, 1998, etc., some additional performance data may be obtained. For example, how much of the credit line increase was used? Did the client go delinquent on the account? What was the current value of the customer? What was their profitability? For example, over the course of a year, twelve (12) sets of performance data may be obtained for this client, each including all of these performance metrics.

L18: Entry 60 of 163 File: USPT Dec 12, 2000

DOCUMENT-IDENTIFIER: US 6158657 A
TITLE: System and method for offering and providing secured credit card products

Detailed Description Text (7):
As illustrated in FIG. 1, output module 200 includes a display 210, a printer device 220, and/or a network interface 230 for receiving the results provided as output from computing module 200. As indicated above, the output from computing platform 300 may include mailing lists of potential customers for credit card products, credit or risk ratings for potential customers, and/or response or potential profitability levels for potential customers. The output from computing platform 300 may be displayed or viewed through display 210 (such as a CRT or LCD) and printer device 220. If needed, network interface 230 may also be provided to facilitate the communication of the results from computer platform 300 over a network (such as a LAN, WAN, intranet or the Internet) to remote or distant locations for further analysis or viewing. In either case, the output from output module 200 can be used by the credit card issuer to generate, for example, the necessary mail offers (which can be either physical or electronic mail offers) for potential customers on the list(s) determined for each secured credit card product. The output from output module 200 can also be used for other purposes, such as internal reports or monitoring.

Detailed Description Text (17):
As illustrated in FIG. 4, the next step in the prospect selection process is to perform a primary risk analysis on the list of potential customers (step S.100). This risk analysis may be performed by computing platform 300 on each potential customer based on a risk model that is particularly suited for individuals with poor or bad credit. Customer and credit-related data may be processed by such a risk model to generate a risk score for each potential customer based on various factors, such as bankruptcy claims, late payment history, payment delinquencies, etc. After determining a risk score for each potential customer, the customers are then divided into groups by computing platform 300 in accordance with their risk scores (step S.110). In this regard, customers may be arranged in groups of risk scores that range from low risk scores to high risk scores. By way of a non-limiting example, computing platform 300 may arrange potential customers into eight different groups of risk scores.

WEST

Generate Collection Print

L23: Entry 13 of 16 File: USPT Feb 23, 1999

DOCUMENT-IDENTIFIER: US 5875236 A
TITLE: Call handling method for credit and fraud management

Detailed Description Text (41):
While any number of customers may be maintained in the Customer Account Table in the NAI database, it may be preferable that only delinquent customers, high risk customers, repetitive delinquent customers, and new customers be maintained in the Customer Account Table. In this manner, thresholding may be implemented for new customers for a brief period (such as three to nine months) to verify that the customer timely pays its bills. If the customer's account is not delinquent at the end of this initial period, then that particular customer may be removed from the Customer Account Table. In contrast, if the particular customer's account has been delinquent, that customer's record status may be changed to credit denied, treatment categories may be modified to allow less usage before alerts are generated, or monitoring may be modified to monitor on a shorter period of time (i.e., weekly rather than monthly).

WEST

Generate Collection | Print

L20: Entry 32 of 54 File: USPT Apr 4, 2000

DOCUMENT-IDENTIFIER: US 6047270 A
TITLE: Apparatus and method for providing account security

Brief Summary Text (11):
While card holders are usually protected by various coverages which shield them from the liabilities associated with the fraudulent use of a card or the corresponding account number, the card issuers, credit, charge and/or debit card issuing companies and/or institutions, and/or their insurance companies, end up paying for the above described thefts and/or fraudulent and/or unauthorized uses. Ultimately, the consumer also shoulders the burden of the costs associated with these thefts and/or fraudulent and/or unauthorized uses in the form of increased prices.

Brief Summary Text (13):
Current practices do not entail and/or do not include the provision for obtaining an authorization, and/or for providing notice to the cardholder before, during and/or shortly after a transaction, which cardholder authorization and/or notification procedure would be helpful and prove to be essential in preventing the fraudulent use and/or unauthorized use of a card and/or the account number corresponding thereto in an unauthorized transaction and/or shortly thereafter an unauthorized transaction has occurred, thereby minimizing the fraudulent and/or unauthorized use of the card and/or the account number corresponding thereto.

Brief Summary Text (46):
The apparatus and method of the present invention provides for the real-time authorization, notification and/or security of financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, electronic money cards, electronic cash cards and/or digital cash cards, which enables a cardholder to monitor, in real-time, all activity involving his or her card(s) and the corresponding account numbers. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost, stolen and/or are or have been fraudulently used, and/or when his or her card number(s) are or have been fraudulently used, and provides an indication to the cardholder of where his or her card(s) are being or have been utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card.

Brief Summary Text (47):
The present invention also provides a means and a mechanism by which to monitor the number of transactions which are unauthorized by the cardholder and determine whether or not to authorize transactions and/or to cancel or to de-activate the card(s). In the above manner, the present invention provides an apparatus and a method to prevent and/or to drastically limit fraudulent and/or unauthorized use of credit cards, charge cards, debit cards, and/or currency or "smart" cards, electronic money cards, electronic cash cards and/or digital cash cards, and/or the account numbers corresponding thereto.

Brief Summary Text (54):
The present invention also provides an apparatus and a method by which to monitor the number of wireless or cellular communication device or telephone transactions, including mobile transactions, which are unauthorized by the wireless, cellular or mobile device telephone owner and to determine whether or not a central processing computer should cancel or de-activate the wireless or cellular device or telephone and/or the account. In the above manner, the present invention provides an apparatus

and a method for preventing and/or for drastically limiting fraudulent use and/or unauthorized use of wireless, cellular, or mobile devices or telephones and/or wireless, cellular, or mobile telephone numbers. The present invention also provides an apparatus and a method for combating wireless or cellular device or telephone "cloning."

Detailed Description Text (38):
The apparatus and method of the present invention provides for the real-time notification of financial transactions involving credit cards, charge cards, debit cards, and/or currency cards, electronic currency cards, "smart" cards and/or telephone account cards which enables a cardholder to monitor, in real-time, activity involving his or her card(s) and the corresponding accounts. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost or stolen, and/or that his or her card(s), and/or the account numbers corresponding thereto, are utilized without his or her authorization and also provides an indication to the cardholder of where his or her card(s) or corresponding account number(s) is being utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card and/or the account.

Detailed Description Text (39):
The present invention also provides a means and a mechanism by which to monitor the number of transactions which are unauthorized by the cardholder and to determine whether or not to authorize transactions and/or cancel or de-activate the card(s) and/or the account. In the above manner, the apparatus and method of the present invention provides an apparatus and a method for preventing and/or for drastically limiting fraudulent and/or unauthorized use of credit cards, charge cards, debit cards, and/or currency or "smart" cards and/or the account numbers corresponding thereto.

Detailed Description Text (201):
The present invention also provides a means and a mechanism by which to monitor the number of cellular or mobile telephone calls and/or transactions which are unauthorized by the cellular telephone owner and to determine whether or not to de-activate the cellular telephone and/or the cellular telephone number and/or account. In the above manner, the apparatus and method of the present invention provides an apparatus and a method to prevent and/or to drastically limit fraudulent and/or unauthorized use of, and/or the "cloning" of, wireless telephones, wireless communication devices, cellular telephones and/or the unauthorized use of cellular telephone numbers.

Detailed Description Text (237):
The present invention also provides a means and a mechanism by which to monitor the number of wireless telephone calls and/or transactions which are unauthorized by the wireless telephone owner and to determine whether or not to de-activate the wireless telephone and/or the wireless telephone number and/or account. In the above manner, the apparatus and method of the present invention provides an apparatus and a method to prevent and/or to drastically limit fraudulent and/or unauthorized use of, and/or the "cloning" of, wireless telephones and/or wireless communication devices and/or the unauthorized use of wireless telephone numbers.

Detailed Description Text (259):
The apparatus and method of the present invention may also be programmable for programmed and/or automatic activation, self-activation, programmed and/or automatic operation and/or self-operation. The apparatus and method of the present invention may provide for an immediate, as well as for a deferred, control, monitoring and/or security function, and/or response thereto, so as to provide for the immediate and/or the deferred control, activation, de-activation, programming, monitoring and/or security, etc., of any one or more the herein described credit cards, charge cards, debit cards, currency cards, "smart" cards, electronic currency cards, banking, brokerage, digital cash and/or financial accounts and associated transaction cards, and/or wireless telephones, wireless communication devices, cellular telephones and/or cellular or mobile communications devices, and/or any other suitable application in and for which the present invention may be utilized.

Detailed Description Text (278):
The present invention may also be utilized so as to provide financial transaction and/or wireless communication device authorization, notification and/or security for any number and/or types of accounts, including credit card accounts, charge card accounts, debit card accounts, currency card accounts, or "smart" card accounts, electronic money or electronic cash accounts and/or other transaction card accounts, financial accounts, brokerage accounts, savings accounts, checking accounts, automated teller machine accounts, wireless or cellular device or telephone accounts and/or wireless or cellular communication device accounts. In this manner, the apparatus may comprise a communication device or communications devices which may receive and/or transmit signals, data and/or information, for any number and/or types of the above accounts, and/or devices, and/or for each of the respective accounts and/or devices utilized, from and to the respective central processing computer and/or central processing computers for the respective accounts and/or devices. In this manner, an individual may utilize a single communication device so as to monitor all of his or her accounts and/or devices and/or types of accounts.

Detailed Description Text (279):
The apparatus and method of the present invention provides for the real-time notification of financial transactions involving credit cards, charge cards, debit cards, currency cards or "smart" cards, electronic money cards, electronic cash cards and/or digital cash cards, which enables a cardholder to monitor, in real-time, activity involving his or her card(s) and the corresponding accounts. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost, stolen, or is being utilized in an unauthorized manner and provides an indication to the cardholder of when and where his or her card(s) is being utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card. The apparatus and method of the present invention provides the same, and/or analogous, features and/or functions for banking, financial, brokerage, electronic and/or digital cash accounts and/or for wireless or cellular device or telephone accounts.

Detailed Description Text (282):
Applicant hereby incorporates by reference herein the following United States patents: U.S. Pat. No. 5,173,594 which teaches a system for printing personalized charge-card service receipts at remote locations; U.S. Pat. No. 5,479,510 which teaches an automated data card payment verification method; U.S. Pat. No. 5,473,667 which teaches a paging system with third party authorization; U.S. Pat. No. 3,723,655 which teaches a credit authorization terminal; U.S. Pat. No. 5,485,510 which teaches a secure credit/debit card authorization; U.S. Pat. No. 5,406,619 which teaches a universal authentication device for use over telephone lines; U.S. Pat. No. 5,444,616 which teaches financial transaction systems and methods utilizing a multireader transaction terminal; U.S. Pat. No. 5,513,250 which teaches telephone based credit card protection; U.S. Pat. No. 4,485,300 which teaches a loss control system; U.S. Pat. No. 4,758,714 which teaches a point-of-sale mechanism; U.S. Pat. No. 4,947,027 which teaches a system for identifying authorized use of credit cards; U.S. Pat. No. 5,357,563 which teaches a data card terminal for receiving authorizations from remote locations; U.S. Pat. No. 5,444,763 which teaches a translation and connection device for radio frequency point of sale transaction system; U.S. Pat. No. 5,243,645 which teaches an automatic system for forwarding of calls; U.S. Pat. No. 3,938,090 which teaches a terminal apparatus; U.S. Pat. No. 5,642,419 which teaches a method for acquiring and revalidating an electronic credential; U.S. Pat. No. 5,621,797 which teaches an electronic ticket presentation and transfer method; U.S. Pat. No. 5,557,518 which teaches trusted agents for open electronic commerce; U.S. Pat. No. 5,455,407 which teaches an electronic-monetary system; U.S. Pat. No. 5,453,601 which teaches an electronic-monetary system; U.S. Pat. No. 5,511,121 which teaches efficient electronic money; U.S. Pat. No. 5,224,162 which teaches an electronic cash system; U.S. Pat. No. 4,977,595 which teaches a method and apparatus for implementing electronic cash; U.S. Pat. No. 5,623,547 which teaches a value transfer system; U.S. Pat. No. 5,438,184 which teaches a method and apparatus for electronic cash transactions; U.S. Pat. No. 5,534,683 which teaches a system for conducting transactions with a multifunctional card having an electronic purse; U.S. Pat. No. 5,521,362 which teaches an electronic purse card having multiple storage memories to prevent fraudulent usage and method therefor; U.S. Pat. No. 5,221,838 which teaches an electronic wallet; U.S. Pat. No. 5,030,806 which teaches a transaction system of the electronic purse type; U.S. Pat.

No. 4,992,646 which teaches a transaction system of the electronic purse type; and U.S. Pat. No. 4,877,950 which teaches an electronic purse device.

WEST

Generate Collection Print

L20: Entry 28 of 54 File: USPT Aug 1, 2000

DOCUMENT-IDENTIFIER: US 6095413 A
TITLE: System and method for enhanced fraud detection in automated electronic credit card processing

Brief Summary Text (3):
The present invention relates generally to credit card verification processes, and specifically to an improved automated system and process for detecting and preventing the fraudulent use of credit cards by unauthorized users.

Brief Summary Text (5):
Credit cards have conventionally been used for financial transactions for reasons of public convenience and economy. Typically, a purchaser merely needs to present the credit card to a vendor to complete a transaction, where all information necessary to complete the financial transaction is contained on the credit card. Credit cards inherently possess a certain degree of risk for fraudulent use, since the credit card information necessary for the financial transaction appears on the face of the credit card. Thus, if a credit card is lost or stolen, an unauthorized user of the credit card may complete financial transactions by merely presenting the credit card number to a vendor. In order to prevent unauthorized use of a credit card, vendors have conventionally asked for picture identification or compared the purchaser's signature with a signature on the card to ensure the purchaser is an authorized user of the card. However, such authorization techniques can only be performed when the purchaser is in the presence of the vendor. Recently, there has been a trend toward performing credit card transactions electronically over computer networks via the "Internet" or phone lines via audiotext systems. In such electronic credit card transactions, the purchaser inputs the credit card information from a remote terminal, such as a computer terminal or telephone keypad, and this information is transmitted to the vendor. Prior authorization techniques used for in-person transactions can not be used with electronic credit card transactions, so new security measures are required to prevent fraudulent and unauthorized electronic credit card transactions.

Brief Summary Text (7):
Another security measure developed to prevent fraudulent electronic credit card transactions is the use of automated number identification (ANI) blocking. Since almost all electronic credit card transactions are performed from remote terminals connected through telephone lines, the vendor automatically collects the telephone number associated with the telephone line of the remote device from the telephone carrier. The vendor possesses a stored list of telephone numbers associated with a pattern of fraudulent use, wherein the ANI collected is compared with the stored list to determine if a match exists. If the ANI collected is on the stored list, then that telephone line is blocked from further use. ANI blocking is effective in preventing continued fraudulent usage of a credit card from a particular phone number. However, ANI blocking is also of limited usefulness, because it correlates a telephone number used on one occasion for a fraudulent credit card transaction as a blocked phone number. Even though the telephone number and credit card are not interrelated, the telephone number will be blocked from any further credit card transactions. The next electronic credit card transaction attempted using that telephone number may be a valid transaction, but the transaction will be denied since the telephone number has been blocked by ANI blocking. Thus, remote terminals frequently having a plurality of different users, such as hotel room telephones or pay phones, will be blocked by ANI blocking by one fraudulent use, preventing subsequent valid credit card transactions from being performed from that remote terminal. While ANI blocking is effective in preventing repeated fraudulent credit card transactions from occurring from the same

remote terminal, it also has the detrimental effect of preventing subsequent valid credit card transactions from being performed from the same remote terminal.

Brief Summary Text (8):
Clearly, there is a need for a method for preventing fraudulent electronic credit card transactions which does not also incidentally prevent subsequent valid credit card transactions from being performed. Moreover, there is a need for a more secure method for preventing fraudulent electronic credit card transactions by requiring identifying data that is not easily attainable by a fraudulent user.

Brief Summary Text (12):
Yet another object of the present invention is to provide a system and method for enhanced fraud detection in automated electronic credit card processing which reduces the number of fraudulent electronic credit card transactions while minimizing the number of valid credit card transactions incidentally prevented from being performed.

Detailed Description Text (8):
By utilizing the information stored in social security number information database 18, the number of fraudulent electronic credit card transactions allowed can be greatly reduced. Credit cards are typically carried by individuals in their wallets, where other information identifying the individuals is also typically placed within the individual's wallet. For instance, most individuals carry their driver's licenses in their wallets. Therefore, if an individual's wallet is lost or stolen, a person coming into possession of the wallet will have access to both the individual's credit card and personal identification. In order to assist in preventing fraudulent usage of a credit card, the present invention requires the user of the credit card to know the social security number of the credit card holder. Since most people do not carry their social security number on their person, this identifying data will not be readily available to a person who fraudulently comes into possession of a credit card number.

Detailed Description Text (10):
Social security number information database 18 and cardholder information database 16 are stored separately from each another and are also accessed separately from each other. If an unauthorized person gains access to credit card information in cardholder information database 16, the unauthorized person will not be able to access the information in social security number information database 18. This prevents the information necessary for authorization of the electronic credit card transaction from being obtained by fraudulently gaining access to one of the information databases. Accessing databases 16 and 18 separately also prevents all of the information necessary for authorization from being obtained if one of the electronic data transmissions is fraudulently intercepted. With the widespread use of on-line computer financial transactions, separate access to databases 16 and 18 is particularly important in preventing fraudulent credit card transactions.

Detailed Description Text (13):
It is also possible for a vendor using electronic credit card processing system 10 of the present invention to limit the amount of expenditures a user may make in a given time period in order to further safeguard against fraudulent transactions. Prior to authorizing the electronic credit card transaction, a threshold check may be performed to ensure that the user has not exceeded a predetermined expenditure limit within a given time period. For example, the user may be limited to certain amount of expenditures each day, each week, each month, etc. The time periods are of the rolling variety where the last given number of days prior to the attempted transaction are monitored for the threshold check. The criteria to be used in each threshold check is determined by the type of goods or services to which the credit card transaction relates. By utilizing an expenditure threshold, the electronic credit card processing system 10 limits the number of fraudulent transactions which may be performed by a user who has obtained all of the necessary information to satisfy the tests for authorization. Placing a limit on the expenditures allowed for an electronic credit card transaction is also useful in preventing "friendly fraud," which occurs when an individual is a valid user of the credit card but has exceeded a limit for the transaction attempted. For instance, where multiple credit cards exist for a certain credit card number, thresholds can be established based on the social security number so that a "global" threshold can be established and upheld for all uses of the credit card. Further, after an electronic credit card transaction has transpired, subsequent

use of the same credit card number may be blocked within a predetermined time period by using the social security number as the variable monitored.

Detailed Description Text (15):
The authorization procedure is substantially the same as the procedure discussed in association with FIG. 2, except step 205 is added where the phone number from which the remote terminal is communicating is automatically collected by central station 12 from the phone provider and stored in memory 22. Further, in step 213, the collected phone number is compared with a list of blocked phone numbers stored in memory 22 which are not authorized to perform electronic credit card transactions. The electronic credit card transaction is rejected in step 208 if the collected phone number matches any of the blocked phone numbers on the stored list. All other steps in the authorization procedure are performed as previously described, and their discussion will be omitted from the description of this authorization procedure. ANI blocking can be useful in preventing continued fraudulent use from a particular phone number known to have a large amount of fraudulent use associated therewith, and ANI blocking may be selectively employed to accomplish this result.

Detailed Description Text (17):
As can be seen from the foregoing, the system and method for enhanced fraud detection in automated electronic credit card processing performed in accordance with the present invention will reduce the number of fraudulent electronic credit card transactions while minimizing the number of valid credit card transactions incidentally prevented from being performed. Moreover, the system and method for enhanced fraud detection in automated electronic credit card processing performed in accordance with the present invention will minimize fraudulent use of a credit card by utilizing identifying social security number data that is not readably attainable or accessible by a fraudulent user.

Detailed Description Text (18):
In each of the above embodiments, the different methods of preventing fraudulent credit card transactions by the electronic credit card processing system of the present invention are described separately in each of the embodiments. However, it is the full intention of the inventors of the present invention that the separate aspects of each embodiment described herein may be combined with the other embodiments described herein. Those skilled in the art will appreciate that various adaptations and modifications of the just-described preferred embodiment can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.